ネットワークシステムにおける標的型攻撃対策の研究

著者	加藤 雅彦
発行年	2015
学位授与大学	筑波大学 (University of Tsukuba)
学位授与年度	2014
報告番号	12102甲第7273号
URL	http://hdl.handle.net/2241/00125871

氏　名（本籍）	加藤　雅彦
学 位 の 種 類	博　士（工学）
学 位 記 番 号	博　甲　第　7273　号
学位授与年月日	平成　27　年　3　月　25　日
学位授与の要件	学位規則第４条第１項該当
審 査 研 究 科	システム情報工学研究科
学位論文題目	ネットワークシステムにおける標的型攻撃対策の研究

主　査	筑波大学　教授	工学博士	岡本　栄司
副　査	筑波大学　准教授	工学博士	片岸　一起
副　査	筑波大学　准教授	博士(工学)	西出　隆志
副　査	筑波大学　助教	博士(理学)	金山　直樹
副　査	東邦大学　講師	博士(工学)	金岡　晃

論　文　の　要　旨

インターネットにおける標的型攻撃は、ネットワークシステムの設計･構築時の不備を巧みに利用しており、深刻な社会問題になっている。そこで、本論文では設計･構築･テスト･実装のシステムライフサイクルを意識して防御に必要な技術を開発した上で、包括的な対策を提案している。

具体的には、第１章の概説の後、第２章では対象となるネットワークシステムとそれらに対してどのような攻撃が行われているかを明らかにし、現状の対策の限界を示している。その上で、第３章では、標的型攻撃を考慮した新たなネットワークシステムの設計手法を提案し、ネットワークシステムのレイヤ内のアクセス情報とレイヤ間の依存関係を明らかにすることで、ネットワークシステム設計における定量評価が可能となることを示し、その応用として攻撃による影響を測る尺度となる脆弱性影響度を提案している。第４章では、段階的に行われる攻撃を想定して、攻撃活動のネットワーク動作をモデリングし、提案ネットワークモデルと合わせることによって、ネットワークシステム上でどのように攻撃が進行するかといったことがシミュレーションできることを示している。そして、第５章で、標的型攻撃の初期段階から使用されるバックドア通信に着目し、プロキシサーバを使ってダミーデータをクライアントに送り込み、その応答を見ることで不正プログラムによる通信かどうかを識別する手法を提案している。その提案手法を実装し、実際に標的型攻撃で使用された不正プログラムを動作させテストを行ったところ、攻撃の初期段階で不正プログラムによる偽装通信を検出することが可能であることが確認され、これにより、早期の攻撃予兆検出が可能であることが示されている。

審　査　の　要　旨

【批評】

近年インターネット環境は重要な情報をやり取りするだけの信頼性を持った社会インフラとなっているが、規模は拡大の一途をたどり、インターネットを支える技術やシステム構成はすでに把握しきれないほどに複雑化している。しかし、ネットワークシステムはいまだにインターネット初期から変わらない手法と技術で作られている。標的型攻撃はそのような従来型の設計・構築方法の限界をまざまざと見せつける進化した攻撃である。このような攻撃に対抗するため、本論文では、設計･構築･テスト･実装のシステムライフサイクルを意識して防御に必要な技術を新たに開発した上で、包括的な対策を提案している。

その提案手法を実装し、実際に標的型攻撃で使用された不正プログラムを動作させテストを行ったところ、攻撃の初期段階で不正プログラムによる偽装通信を検出することが可能であることが確認されており、これにより、早期の攻撃予兆検出が可能であることが示されている。この結果は今後のネットワークセキュリティにおいて、極めて有用である。

以上により、本論文は博士論文にふさわしいと認められる。

【最終試験の結果】

平成 27 年 1 月 27 日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。この結果とリスク工学専攻における達成度評価による結果に基づき、学位論文審査委員全員によって、合格と判定された。

【結論】

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。